

Incydr™ + Ping

SSO-powered context for smarter security

Mimecast Incydr integrates with Ping Identity to perform authentication and provisioning as well as to ingest and leverage user context to inform risk prioritization.

Integration Overview

Ping Identity provides Incydr with user attributes including division, manager, title or location to enhance monitoring of users most likely to put data at risk, such as contractors or departing employees. This approach gives organizations flexibility to create and customize their Incydr environment based on needs for security, scalability, employee productivity and user management.

Benefits

Data protection: Protect data by applying access controls in response to detected threats

Complete context: Utilize user attributes to provide quick context and speed decision-making during an investigation

Increase productivity: Effectively monitor and mitigate Insider Threats by automating Watchlist management of high-value data

Features

Single Sign-on

Implement single sign-on (SSO) as the authentication method in your Incydr environment to simplify the user experience while ensuring data is secure

Watchlist Management:

Use Ping Identity information such as department, manager, title, and location to complete a user's profile within Incydr and to automate the employees who should be added and removed from Watchlists

